series base no./vol./reissue
N-24879 /001/00
author Karl Auerbach
date 15 January 1980

NOTE an internal working paper

System Development Corporation
2500 Colorado Avenue • Santa Monica, California 90406

AN INTRODUCTION TO THE CONCEPTS OF INFORMATION REGULATION AND DATA PROTECTION

AN INTRODUCTION TO THE CONCEPTS OF INFORMATION REGULATION AND DATA PROTECTION

Karl Auerbach
SYSTEM DEVELOPMENT CORPORATION

ABSTRACT

The reader is introduced to the definition of "data protection" as that body of rules governing the handling of "name-linked" information. The relation of data protection to privacy, defamation is discussed. The competing policies and principles of fair information practices are described with reference to the issues of transborder data flow. Elements common to most data protection regimes are isolated and described along with arguments supporting various positions on unresolved issues. The relevance of data protection to the information handling industry in general and SDC in particular is noted. The legal basis upon which civil lawsuits against SDC could arise and succeed are listed. It is pointed out that SDC presently has no policy or procedures designed to prevent data protection violations. A recommendation is made to implement such policies and procedures.

CONTENTS

AN INTRODUCTION TO THE CONCEPTS OF INFORMATION REGULATION AND DATA PROTECTION

Karl Auerbach
SYSTEM DEVELOPMENT CORPORATION

January 15, 1980

This note attempts to give the reader an introduction to the subject of "data protection" and to indicate the relevance of data protection to the information industry and SDC. The discussion found here is rather general -- there are few references to specific data protection regimes. Subsequent notes in this series will focus more closely on existing and foreseeable data protection and information measures in the United States and elsewhere.

Other notes in this series will focus more deeply upon how organizations such as SDC and the individuals employed by such organizations will be affected by data protection rules and what measures should be taken to ease the strain of compliance.

1. OVERVIEW AND SUMMARY

Data protection is a very complex topic. Its essence is the "proper handling" of information. Information is "properly handled" when the interests and desires of the subject of the information are given consideration and weight when collecting, using, storing, disseminating, and destroying that information.

There are few presently existing bodies of data protection regulation. However, it is certain that many new rules are forthcoming from legislatures in the United States and abroad. These rules will affect all information handling practices. Considering that the institutions of modern society and business are information intensive, the effects of data protection may be as profound as those brought about by labor and environmental legislation.

Especially complex issues arise where multiple, and potentially conflicting, data protection regimes apply or where information is being moved between separate regimes.

Data protection rules will be rules of law. Failure to comply may result in regulatory sanctions and legal liability to customers and third parties.

SDC will be directly and strongly affected by data protection rules. Like other companies, SDC's internal record-keeping policies will have to be modified. In addition, because SDC is in the business of providing information handling services, products, and systems, SDC will have to ensure that data protection requirements are imposed upon those services, products, and systems.

At the present time SDC has not made any substantive steps to ensure that data protection requirements are in-fact incorporated into corporate policies, services, products, and systems as those requirements become law. As a consequence, SDC may suddenly find its services, products, and systems unmarketable and its internal policies invalidated. The corporation is taking a large and un-calculated risk.

SDC must begin to ensure that all of its internal policies and procedures, all of its products and services, and all of its proposals and delivered systems are consistant with forthcoming legislation. A centralized corporate function should be established to monitor compliance, educate corporate personnel, and keep abreast of new developments.

2. WHAT IS DATA PROTECTION?

Data protection consists of that body of rules governing the collection, validation, processing, storage, distribution, and destruction of name-linked information. Name-linked data is data which can be related, directly, indirectly, or inferentially to either a specific person, a well-defined group of people, or a legal entity (i.e. a juristic person). Such rules may be mandatory or "voluntary" and may be promulgated by governmental bodies or information industry trade organizations.

As yet, most regulation is imposed upon name-linked data only. Other data is left relatively uncontrolled. Existing (and proposed) laws and conventions on copyrights, patents, trade-secrets in conjunction with contract and licensing laws provide a the holder of non-name-linked information with a semblance of control. Export restrictions, mild taxation, and "technology transfer" requirements have often been imposed on non-name-linked information by national governments. The former two methods are tools of well developed nations to restrict technology outflow. The latter method is used by underdeveloped nations to induce technology inflow.

Legislative activity has been fairly intensive in the United States and abroad. Numerous committees are examining the problems, bills are pending before legislatures, and statutes are being enacted into law. Prior to 1970 no data protection laws were in effect. Today the list of countries and international organizations which are discussing and legislating or which have enacted data protection laws include:[1]

1. The United States:
   a. Federal government
   b. California
   c. Arkansas
   d. Indiana
   e. Minnesota
   f. Ohio
   g. Maine
   h. Michigan
   i. Utah
   j. Virginia
   k. Pennsylvania
   l. Oregon
2. Canada
   a. National government
   b. Various provinces.
3. Germany
   a. Federal government
   b. Hesse
   c. Rhineland Palatinate
4. The United Kingdom
5. France
6. Sweden
7. Switzerland
   a. Federal government
   b. Geneva Canton
8. Spain
9. Portugal
10. Italy
11. Denmark
    a. Federal government
    b. Faroe Islands
12. Norway
13. Belgium
14. Austria
15. Luxembourg
16. Greenland
17. The Netherlands
18. Japan
19. New Zealand
20. Australia
    a. Federal government
    b. New South Wales
21. The Council of Europe (Twenty-one member nations.)
22. The Organization for Economic Co-operation and Development (OECD) (Membership consists of most of the Council of Europe members plus the United States, Canada, Australia, New Zealand, and Japan.)

Data protection is a matter of international scope. As yet, however, most legislation has been at the national (or sub-national) level.

Why has data protection become of such interest recently? Although computers have been around since the early 1950's it is only within the last few years that it has become feasible to cheaply store and quickly access huge

1. The list was compiled in November 1979. There is presently a great deal of legislative activity. As a result, the list rapidly becomes out-of-date.

quantities of data and to combine separate computers into an efficient network permitting the corrolation of personal data. Moreover, the technology of the information industry is so complex, new, and ever-changing as to be seemingly beyond the comprehension of all but a small elite cadre (or oligarchy) of information technologists.

It is difficult to compile an imposing list of perfected data protection violations. "The desire to legislate has on the whole been based less on the experience of abuses than on the desire to prevent abuses in the future and to influence developments before they become irreversible."[2]

"Privacy" and "defamation" are not synonomous with "data protection". Rather, the three concepts partially overlap. Data protection is concerned with the handling of name-linked information. Data protection rules govern information whether or not it is obtained from a data subject who knowingly gives his consent. In the United States the term "privacy" has two meanings. In one sense, "privacy" refers to the present concern for fair information practices as expressed by the Privacy Act of 1974,[3] the Fair Credit Reporting Act[4], the Report of the Privacy Protection Study Commission, the California Information Practices Act of 1977[5], and the like. In this sense "privacy" is very closly tied to "data protection", although its scope is perhaps a bit less broad. In the other sense "privacy" refers to the common law tort often called "invasion of privacy". In this sense "privacy" is concerned with intrusions and with publications of truthful information which places the data-subject in a "false-light" or which would be offensive and objectionable to a person of ordinary and reasonable sensibilities.[6] Defamation is concerned with the publication of untruthful information which tends to bring the data subject into disrepute.[7]

In the United States the areas of privacy and defamation are subject to a mass of complex rules based upon the first amendment protections of speech and the press.[8] There is a strong possibility that, in the United States, data

2. G. Stadler, "Survey of National Data Protection Legislation", Computer Networks, June 1979, Volume 3, Number 3, page 174.
3. PL 93-579
4. PL 91-508
5. California Civil Code, sections 1798 et seq.
6. William L. Prosser, Handbook of The Law of Torts, fourth edition, 1971
7. ibid.

protection will also be subject to similar constitutionally based rules.

Each social system has its own notion of what constitutes a "reasonable expection of privacy". Even between such outwardly similar societies as the United States and the United Kingdom there are substantial differences between personal sensitivity towards salary, medical, and employment information.[9] In Japan personal tax returns are generally available by law for public examination.

Data protection, unlike either privacy or defamation includes the notion of a "balance of information power". Increased access to information, although not intrusive in a privacy sense, represents a loss of control or a reduction in bargaining power by the data subject.

2.1 TERMINOLOGY There are a few words used in the data protection area which ought to be defined:

1. Data subject: A data subject is the person or legal person about whom the data relates.
2. User: A user is someone who uses the data.
3. Record keeper: A record keeper is someone who maintains or records the data.
4. Data Bureau: A data bureau is a supplier of labor or computers used by the record keeper to maintain records.
5. Record or File: A record or file is a single collection of data or information relating to a data subject. The various parts of the record or file may be physically scattered among a number of computers or filing systems maintained by the record keeper.
6. Universal Personal Identifier: A universal personal identifier is a unique "name" associated with a specific individual.
7. Information or Data: In this note no distinction is made between the meaning of the words "data" and "information".

2.2 PRINCIPLES OF FAIR INFORMATION PRACTICE Data protection is often defined in terms of "fair" information handling. Various sets of of these "fair information practice" principles have been formulated. Two such sets of

8. New York Times Co. v. Sullivan, 376 US 254 (1964), motion denied 376 US 967.
Numerous cases since 1964 have expanded the meaning of the first amendment.

9. M.D. Kirby, "Data Protection and Law Reform", Computer Networks, June 1979, Volume 3, Number 3, page 149 citing D. Firnberg, "Computers and Privacy", Cantor Lectures, 1977, I, 3.

interest are those proposed in the UK by the 1972 Younger Committee[10] and in the US by the 1973 report of the US Department of Health, Education, and Welfare's Secretary's Advisory Committee on Automated Personal Data Systems.[11]

The Younger Committee's Principles

1. Information should be regarded as held for a specific purpose and not be used, without appropriate authorisation, for other purposes.
2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
3. The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.
4. In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
5. There should be arrangements whereby the subject could be told about the information held concerning him.
6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.
7. A monitoring system should be provided to facilitate the detection of any violation of the security system.
8. In the design of information systems, periods should be specified beyond which the information should not be retained.
9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
10. Care should be taken in the coding of value judgements.

The Secretary's Advisory Committee's Principles[12]

1. There must be no personal-data record-keeping system whose very existance is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

10. Report of the Committee on Privacy, 1972, Cmnd 5012.
11. US Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, 1973.
12. These principles have been "refined" into eight principles listed at page 501 in Personal Privacy in an Information Society, the Report of the Privacy Protection Study Commission, July 1977. It is not worth restating them here as they have little additional content.

2.3 DERIVATION OF DATA PROTECTION RULES Data protection rules are the result of a political process in which many factors are balanced:

1. Privacy -- A conception that modern information systems are, or have the potential to be, overly instrusive is a major force behind data protection rules. There is a simple fear that computerized information casts a "false light" upon an individual -- that the information is an inaccurate, incomplete portrayal of the "real" person. Finally, there is the fear that once a data subject discloses, for some limited purpose, some sensitive information that the information will be flashed, without control, to computers across the world to be used at an unknown future time for an unknown purpose.

   In many jurisdictions, "privacy" has become a constitutional right. In California, Spain, and Portugal the right to personal privacy is (or will shortly be) expressly granted by their constitutions. In the United States a right of privacy of sorts has been derived from the Federal Constitution.[13] I believe also, that the rarely used "privileges or immunities" clause of the Fourteenth amendment of the US constitution can someday be the basis of a constitutional right to privacy.

   Privacy includes the privilege of individuals to hide their past transgressions in order to "make a fresh start" with a "clean slate". This notion leads to restrictions on the use of data which is sufficiently old as to be of questionable relevance to the present.

2. Social values of free information flow -- There is a social value in free flows of information. For example, medical record information can be quite useful in the detection and control of epidemics and carriers of communicable diseases.

3. Freedom of governmental information -- In the interest of open government and an informed electorate many countries have laws which allow access to governmental records unless a specific exemption exists.

4. Commodity value -- Because information is a commodity capable of being bought and sold, there is a need to establish trade rules applicable to the special characteristics of information.

13. Griswold v. Connecicut, 381 US 479 (1965)
Roe v. Wade, 410 US 113 (1973)

5. Trade protection -- Data protection rules can be an effective tool for a nation to protect its own information industry. By restricting the ability of companies to transfer information across the nation's borders, the nation can induce those companies to establish or use local data processing facilities. For obvious reasons, this factor is not discussed by those nations which use it.

6. National sovereignty -- Information is power. A nation loses some of its sovereign powers when it does not have control over information concerning its citizens and when it can not prevent the use of such information by other countries. These are particularly strong considerations in many European and third-world countries. The third-world countries are faced with the dilemma that if they restrain the flow of information about their citizens, then they can not effectively argue for greater sharing of worldwide (especially developed nations') information resources.

7. Fear -- Much of the data protection activity is driven by a Luddite-like fear of technology. "[T]he law must have an increasing role in re-asserting against the scientist and technologist standards which society counts as important."[14]

8. Individual self-determination -- Institutions and legal entities (corporations, etc.) inherently have more power than individuals. Many aspects of data protection rules are intended to provide affected individuals with some means of affecting decisions made about them.

9. Constitutional limitations -- In many instances data protection rules are structured to conform with some constitutional restriction upon the powers of the promulgating authority.

2.4 TRANSBORDER ISSUES A body of data protection rules acts only within the jurisdiction of the promulgating authority. (This jurisdiction may extend beyond the geographic scope of the authority, however. For example, US laws may apply to US citizens wherever they may be. US citizens are subject to the US internal revenue code even when living and working abroad.) The term "transborder data flow" encompasses many of the issues arising from this regionalization of regulation. There is a potential for conflict between rules at borders between data protection jurisdictions. There could be a

14. This quote is taken from, but probably does not represent the views of M.D. Kirby, "Data Protection and Law Reform", Computer Networks, June 1979, Volume 3, Number 3, page 149.

direct mutual exclusion as for example if the United States requires transmitted data to be enciphered and the United Kingdom requires clear text. There could also be situations where country A's standards require country B to "upgrade" (perhaps unwillingly) to A's standard.

Where there exist countries or jurisdictions where the protection is less than elsewhere, there exists the potential of "data havens". A data haven is to information what Liberia and Panama are to ships and what Delaware is to US corporations -- a place where regulation is less burdensome or intrusive.

The low (and decreasing) cost of information transport allows record keepers to avoid stringent data protection restraints. Jurisdictions can, to some extent, prevent record keepers from using data havens by limiting the flow of information into such countries. Consequently many countries have imposed rules which do not permit the export of name-linked information unless certain conditions are met. The usual condition is that the receiving country provide an "equivalent" degree of protection.

The question of "equivalancy" is likely to cause considerable trouble for multi-national corporations. The effective operation and management of multi-nationals depends upon their ability to quickly gather and act upon information. Export of data may be blocked unless the data protection agency of the exporting country can be convinced that the receiving country provides equivalent protection. Resolution of the question of equivalency may center around whether both countries have regulatory agencies, whether both the public and private sectors are subject to regulation, whether similar rules apply to both the public and private sectors, and whether the rules apply to all name-linked data or only to data on citizens to the exclusion of aliens or corporations.

The Swedish Data Inspection Board (DIB) has, at times refused permission for Swedish organizations to export data to the UK for processing. The Swedish DIB has also, at times, prevented the export of personal data from Swedish subsidiaries of US firms to their parent companies in the US. Canadian subsidiaries of US companies are being pressured to establish Canadian sites for their databases in order to avoid sending information on Canadian citizens to the US for processing by the parent company.[15]

15. Sir Norman Lindop, chairman, Report of the Committee on Data Protection, October 1978, Cmnd. 7341. Section 4.58.

Restrictions on information flow will force multi-national corporations to de-centralize their operational structures along the lines of national frontiers.

The United States is in a particularly poor posture regarding the issue of "equivalency". The US approach to data protection is sufficiently different from that of most other countries, that equivalency arguments will be difficult to make. For example, the United States tends to apply specific regulation to very specific activities, leaving enforcement to individual civil lawsuits. Most other countries apply broad principles through an administrative enforcement agency.

Apparently the US is already suffering from reduced information flows.[16] The US Food and Drug Administration (FDA) will not allow certain new drugs to be tested on humans in this country. Many European countries do permit such testing. (Those countries are, in a sense, a drug testing haven.) In order for the test results to be useful they must contain a large number of intimate personal facts. As a result the data protection boards of the countries in which the testing occurred will not allow the data to be exported to the US. This export ban prevents the drug companies from presenting evidence to the FDA supporting use of the drug in the US.

There is a very strong possibility that an international data protection convention or treaty will be drafted in the next few years. Many researchers and commentators working on international infomation flow matters, as well as international organizations, such as the OECD and Council of Europe, have recognized the need for conformity.

2.5 MULTIPLE JURISDICTION ISSUES In Federal countries such as the United States, there exists the possibility that jurisdictions overlap. For example, here in the US there are very few areas in which Federal of state law acts to the total exclusion of the other.[17]

In the United States the Federal government has the ability to pre-empt state activity in certain areas if Congress (or in some instances, the Supreme Court) decides to do so. Pre-emption is used principally to impose uniform rules upon interstate commerce in order to avoid multiple, inconsistant burdens upon concerns engaged in interstate commerce. In the absence of express

16. This story comes from Roy Gates and has not been verified.
17. National League of Cities v. Usery, 426 US 833 (1976)

pre-emption, a complex and vague set of rules apply to determine whether state of Federal law (or both) applies to a given event. Thus a company may not be able to know to a certainty what rules govern its handling of sensitive information.

State borders mean little to the information industry. Networks span the entire country. Yet the Federal government has, as yet, not exercised its pre-emption powers to impose a uniform data protection law.

The United States Constitution provides that treaties and congressional statutes are of equal stature and effect.[18] A treaty may regulate activities which would otherwise be beyond the power of the Federal government.[19] Consequently, if an international convention is adopted and the United States becomes a signatory, and the Senate gives its advice and consent, then there may well be an international law of data protection applicable to all activities in the United States.

3. CHARACTERISTICS OF DATA PROTECTION RULES

The remainder of this note describes the building blocks used to construct data protection rules. Usually not all of the aspects mentioned below are included. Actual rules usually contain complex exceptions, exclusions, and conditions.

3.1 WHO IS THE PROTECTED DATA SUBJECT? Data protection rules govern only records containing data which can be linked to some individual, class of individuals, or legal entity. Not all name-linked data need be regulated. Rather regulation may be limited only to that information linked to certain classes of data subjects. Information relating to different classes of data subjects may be regulated in different ways. Certain data-subject may not be protected at all.

1. Most bodies of data protection rules address, in one way or another, information which can be name-linked to individual people. However, the operation of these rules may be affected by the status of a person. Information about a "citizen" or "resident" may be treated differently

18. Article VI, paragraph 2. "This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the constitution or Laws of any State to the Contrary notwithstanding."

19. Missouri vs. Holland, 252 US 416 (1920)

(usually given more protection) than information about "aliens" (who may be completely unprotected).

Accurate identification of the data subject can be difficult. Personal names are not unique. The telephone directory for the western section of Los Angeles has twenty-six entries for "Rob[er]t Johnson". A unique personal identifier would be a great boon for making correct linkages between information and people. There would be a large social benefit if information could always be attached to the correct individual (and vice versa). Detrimental information wouldn't end up harming a person who shares the same (or similar) name. Medical records could be accurately retrieved in an emergency. However, a unique universal identifier induces fears of an Orwellian "Big Brother" and of becoming a "number" rather than a "person". The 1977 Constitution of Portugal expressly prohibits all purpose indentification numbers for individuals.

2. Data protection rules may cover juristic persons. A juristic person is a legal entity such as a partnership, corporation, foundation, or church. Whether or not such legal entities should be protected data subjects is an issue of much debate. Separating the arguments into the two opposing camps we have:[20]

PRO --

- Legal entities (mainly profit making corporations) are usually set up for competitive purposes. Some degree of secrecy is necessary for competition to work.

- Data protection rules seek to regulate the flow of information in order to ensure that those who need information for lawful and reputable purposes can get it freely, while those who do not cannot get it unless the data subject is willing to give it to them. In that context, there may be all kinds of information about bodies and associations which others may or may not need for lawful and reputable purposes. For example, the finances of a tennis club will be matters of legitimate concern for its members, its bank manager, and the tax collector, but not necessarily or always for everyone else in the country.

20. Many of the following arguments were adopted (often lifted verbatim) from Sir Norman Lindop, chairman, Report of the Committee on Data Protection, October 1978, Cmnd. 7341. Sections 18.31-18.44

- Collective entities can sometimes be as vulnerable to information abuse as individuals; for instance a wrong or misleading credit rating can do as much harm to a trading company as to an individual.

- Information about bodies and associations can often be related to individuals, in that information about a group may carry with it implications about its members. A significant inference could be drawn from the fact that the golf club to which a person belongs charges high subscriptions, or that a society of which he is a member has distinctive political aims. Again, a list of companies prepared by reference to the race, color, creed, or political complexion of their directors could have serious implications for those directors' privacy.

CON --

- Privacy is essentially something personal, something for which individuals have a desire, or claim a right. It would seem odd if an incorporated company could claim "privacy" for information about itself.

- Corporations are entities which the society allows to exist. Since these entitles are merely creations of the society, they have no "expectation of privacy" as does an individual. Moreover, the general public is entitled to know a good deal more about the affairs of bodies and associations than about those of individuals, principally because such bodies tend to exercise over others more power, both economic and political, than individuals do on their own. Over the years it has been thought wise to require corporations to make more and more public disclosures of their operations, dealings, and financial conditions. Thus it is, inappropriate to give corporations the full panapoly of protection. It is, however, appropriate to provide such entities a limited protection in the form of trade secrets, copyrights, patents, and restrictions on whether government agencies are permitted to disclose information they have coerced from the entity. Such entities can make their own private law in contracts and agreements they make when they

disclose information to other non-governmental entities.

- Most data protection rules afford a data subject the right to inspect records held by a record keeper pertaining to that data subject. When the data subject is a legal entity (e.g. a profit making corporation) there is the potential for violation of the record keeper's privacy. This occurs because the mere fact that the record keeper is maintaining information on the data subject implies something about the record keeper's competitive posture or activities. For example, suppose that an toy company produces, among other things, a "Wizbang". The toy company may be able to corroborate rumors that a competitor plans to introduce a product to compete against the "Wizbang" by asking that competitor to disclose all records it has on the toy company. If the toy company finds that the competitor has extensive records concerning the sales performance of the "Wizbang" but very few on other products of the toy company then the toy company can infer that the competitor is interested in the "Wizbang" business. Additional information about the record keeper can be gleaned from the nature of the information held in the record itself. This is especially true if the record is some sort of industry wide composite or planning document.

Rather than providing collective entities with the full panapoly of protections afforded to a human data-subject, a compromise position will probably be adopted. One possible approach to a compromise is to provide individuals with a broad privacy right subject to a few express exceptions. On the other hand, collective entities would have no privacy rights except those expressly granted. The outcome of the debate over the nature of the protection to be afforded to collective entities is far from certain . Corporations and other collective entities have not, as yet, made much effort to develop and support their positions.

3.2 WHAT IS THE NATURE OF THE INFORMATION? The affect of a data protection rule may depend upon the nature of the information contained within a record.

1. A rule may govern only that information which is, or the disclosure of which would be, an "obvious" violation of personal privacy.
2. Often especially stringent rules apply to information pertaining to

certain activities. In particular some countries prohibit the collection and use of name-linked information about an individual's religious, political, labor union activities, arrest record, racial origin, or philosophical views without the data subject's consent or statutory authority.

3. Special prohibitions may be accorded to data which came from another country which has more stringent rules.
4. There are many rules which cover "statistical information". A statistical database is a database which contains no apparent link between the information and the name of the data-subject. Simple, well-known techniques are available to extract name-linked data from many statistical databases. A body of rules has been developed to ensure that it is difficult to extract such information from a statistical database.

3.3 WHAT ARE THE RIGHTS OF THE DATA SUBJECT? A body of data protection rules may allow the data subject certain rights of access and challenge with respect to the information.

1. A record keeper may have to publish a notice to inform the public that it is operating a system of records. This notice will probably have to contain information about the type of information found in the system and the procedures the record keeper follows. The intent of these disclosures is to allow data subjects to learn the existance of systems which may contain information concerning them and to quickly determine whether there is reason to be fearful of an improper use of the information.

   In some instances all data subjects on which a record keeper has files must be given actual notice, either when a record is first created or periodically. A first-class letter is often a sufficient vehicle for such notice.

2. A data-subject may be accorded the right to inspect the records relating to him. (With respect to the US Fair Credit Reporting Act, a teapot tempest has occurred over whether the data subject has the right to inspect the information in a complete and comprehensible form or merely to be given a description of the "nature and content" of the record.)

   If the data-subject disagrees with what he finds in the record he may have the right to challenge the accuracy of the record. The record keeper may be then required to perform a validation procedure. If the information is found inaccurate, it may have to be expunged. If the information is not found inaccurate and the data subject still disagrees,

the data subject may have the right to insert a statement of his viewpoint. If the record is altered or expunged because of an inaccuracy or if the user inserts a statement, the record keeper may be required to forward an updated copy to all past recipients of the record. These past recipients may be required, in turn, to forward updated copies to anyone to whom they disseminated the information.

In the US it seems to be an axiom that an individual "shall have the right to see and copy"[21] information pertaining to him. In the UK a different attitude prevails. The UK Data Protection Committee concluded that what is important is that information be properly handled. In some instances data-subject access is an appropriate means to check whether data is indeed being properly handled. However, instances are conceivable where data-subject access is socially unproductive and other forms of supervision are more appropriate.

In many instances there may be fairly short time limits in which the record keeper must respond to the data subject. The record keeper may often be allowed to charge the data subject a fee reflecting the actual cost of assembling and providing the record. However, the costs of re-verification, update, and re-distribution will probably have to be borne by the record keeper.

3.4 WHO IS THE RECORD KEEPER? Different rules may be applied to different classes of record keepers. Usually a major distinction is made between "private" and "public" (i.e. governmental) activities. Unfortunately, such a distinction is not universally useful -- the states of the United States and the nations of the world have no consistant standard classification of activities into either "public" or "private". The French even have the category "administrative" (which brings to mind the old saying that France is administered, not governed.)

1. Public sector users
   a. The governing rules may vary by the user's branch of government or agency. For example, in the United States only executive agencies are subject to the guidelines found in Office of Management and Budget (OMB) circular memorandum A-71.
   b. Different rules may apply depending whether the user is part of a

21. See the second modified principle, at page 501 in Personal Privacy in an Information Society, the Report of the Privacy Protection Study Commission, July 1977.

state or federal body. Again using the United States as an example, California agencies are constrained by the California constitution, California statutes, and executive orders while the US Privacy Act of 1974 affects only Federal agencies.

c. Often a single, uniform rule covers all public agencies. However, in many instances specific agencies, or specific activities are singled out for special regulation. When a public agency is acting in a quasi-private activity (especially those listed under "Private Sector", below) it may be treated as a private sector user.

Activites which often come under special data protection rules include:

- Police and security services.
- Tax collection agencies.
- Welfare dispensing agencies.
- Public health services.
- Census
- Public educational institutions

2. Private sector users

a. The entire private sector may be subject to broad data protection rules. Many European countries adopt this approach.

b. Specific private activities may be subject to specific sets of data protection rules. Some activities which have been singled out include:

- Medical record keeping.
- Employee record keeping.
- Financial and banking.
- Consumer credit granting and credit verification.
- Electronic Funds Transfer
- Insurance
- Private education
- Direct marketing

3. Some sets of rules except manually maintained information from their operation. Since one of the major reasons that data protection is now evolving so rapidly is the fear that computers are going to take over the world, many rules exempt manual systems. It is felt that manual systems have existed for a long time without causing anyone undue distress. It is recognized by some, however, that there is a fine line between a manual system and a computerized system which simply uses paper as a storage medium. If a paper system contains a computerized filing, indexing, and searching mechanism, the speed of retrieval and amount of information which can be contained in the system approaches (and may even exceed) that of a purely automatic system. In addition, it is difficult to adequately define the terms "computer" and "automatic".

The argument has been made that inclusion of manual systems will add so much overhead that manual systems will become uneconomic. This will be a major hinderence to small business activities who will find that their their record keeping costs are greatly increased.

As one example of what can happen if manual systems are excluded from coverage, consider this anecdote:[22] Swedish banks have been refused permission to keep a computer file of persons known to have committed crimes against banking institutions. Consequently, the banks have simply created a manual card file to replace the prohibited computer file. (The Swedish Data Inspection Board aids such systems by permitting a computerized record to point to, or at least flag the existance of, a corresponding manual/paper record.)

3.5 THIRD PARTY ACCESS Many data protection rules provide means for third party access to name-linked data.

1. The provisions usually allow auditors to inspect the system to determine whether the system is operating properly. The auditors are permitted to disclose the results of their audit, but not to disclose any name-linked data. (It is interesting to note that the Privacy of Electronic Fund Transfer Act of 1979 presently before the United States Congress makes it arguably illegal for bank auditors to inspect EFT systems.[23])
2. A record keeper may be allowed (or required) to disclose name-linked information to police if there is an indication of criminal activity.
3. Police may be able to obtain access through an appropriate procedure, usually requiring a disinterested judge to determine whether the police have a sufficiently reasonal basis for their suspicion that criminal activity has or is occurring.
4. Litigants in a civil action may be permitted access to relevant records pertaining to other litigants and, perhaps, witnesses.

Where an access is made without authorization, the various "computer crime" laws come into play. The basic model for computer crime laws is that it is improper for a person to access, or attempt to access, information without authorization or without a proper purpose. It is not relevant whether that information is name-linked. This note will not further delve into the topic

22. Sir Norman Lindop, chairman, Report of the Committee on Data Protection, October 1978, Cmnd. 7341. Section 14.14

23. HR 5560 (96th Congress, 1st Session)

of computer crime except to note that criminal penalties may be imposed for certain violations of data protection laws.

3.6 RECORD KEEPER AND DATA BUREAU RESPONSIBILITIES The rules will certainly say something about the manner in which record keepers and data bureaux must manage records.

The fair information practices principles listed in section 1.2, above, have an impact upon the way name-linked information is collected, used, and disseminated. Following is a list composed of responsibilities which may be imposed upon a record keeper or data bureau. The list was compiled from various US and foreign data protection laws, both existing and proposed.

1. Collection restrictions
   a. A data subject may have to be informed that information concerning him is being collected, even if it is being collected from a third party.
   b. Data subject may have to informed of his rights regarding the information being collected.
   c. Data subject may have to be told of the use for which the information is being collected.
   d. Data may have to be obtained directly from- or be verified by- the data subject.
   e. Only that information reasonably needed and reasonably relevant to the announced purpose of the data collector may be collected.
   f. Data gathering techniques may have to be designed to ensure maximum accuracy. Validation of data may be necessary.
   g. "Pretext" interviews may be prohibited. (A pretext interview occurs when a data collector gathers information for one purpose while purporting to be gathering information for another purpose.)
   h. The encoding of value judgements may be prohibited or subject to safeguards. One suggested safeguard requires the judgement to be labeled as "fact", "unverified factual assertion", or "subjective judgement". In the latter case, the name of the person who made the judgement, perhaps along with a short summary of reasons, should be recorded along with the data.[24]

2. Usage restrictions

24. Sir Norman Lindop, chairman, Report of the Committee on Data Protection, October 1978, Cmnd. 7341. Section 5.44

a. Data may have to be used only for the purpose for which it was collected.

b. Data may be limited to purposes "not inconsistant" with that for which it was collected.

c. Security measures may be imposed. There may be an affirmative duty to guard against or report violations of security.

d. Information older than a certain age may have to be eliminated. A "timeliness" requirement, rather than a specific period, may be imposed.

e. Certain information may not be used for certain purposes. For example, arrest records may not be used for employment decisions.

f. Information may have to be "complete" before it is allowed to be used.

3. Transfer restrictions

a. Limits on the extent of dissemination may be imposed.

b. The data subject or a data protection authority may have to be notified- and may have to approve- of any dissemination.

c. Any updates or data subject challenges may have to be forwarded to past and future recipients. This implies that a record keeper may have to maintain distribution lists for each record. The burdensome aspects of this requirement have been eased somewhat in proposed US laws which require a record keeper to send updates only to those recipients which the record keeper has a reason to believe have received an inaccurate copy.

4. Data destruction

A. The record keeper may be required to ensure that when data is destroyed for one purpose or another, that such data is eliminated from all storage media. Procedures will be necessary to prevent re-introduction of such data from archival storage.

B. Notice of destruction may have to be sent to all past recepients of the record.

5. General restrictions

a. Data subject notification may have to be direct (by first-class mail, telephone, or legal process) or indirect (by publication in a newspaper or registry.)

b. Personal may have to be certified- or licensed- by an independant

authority.

c. All actions of a data collector, record keeper, or data bureau may have to be registered with a data protection authority. The registration statement may have to contain extensive details on the record keeper's or data bureau's operations, databases, and future plans. The registry may or may not be available for public inspection.

d. Prior approval or license may have to be obtained from a data protection authority. As above, a detailed application may be demanded by the authority and may be made public.

e. All phases of information handling may be subjected to third-party audits and spot-checks for compliance and accuracy.

f. Taxes may be imposed upon certain practices or types of data. Such taxes may be designed merely as revenue measures or as a means of making undesirable practices economically impractical.

g. Record keepers and data bureaux may be constrained to deal only with "approved" subcontractors.

h. All hardware and software, whether produced in-house or purchased, may have to have be certified by an independent certification authority before it may be used.

3.7 FORMS OF DATA PROTECTION RULES The rules may regulate information handling in a number of ways. Many of the rules may contain a number of positive ("X shall do Y") and negative ("X shall not do Y") provisions. In many instances a unified body of data protection rules will be constructed using a number of the forms found in the following list.

1. Statutory requirements
2. Administrative rules
3. Codes of practice on a per-industry basis. (These may be promulgated by either a governmental agency or a private trade association.)
4. Mandated contractual duties -- A government may require the insertion of certain terms into contracts it makes with record keepers and data bureaux imposing upon those record keepers and data bureaux (and their sub-contractors) certain information practices regarding third-party data subjects.

3.8 SCOPE OF EFFECT A jurisdiction promulgating a data protection rule may chose to give it a narrow or broad scope of effect. In the UK it has been

recommended "that the statute should bite on any part of a data handling activity which takes place in the UK, irrespective of the nationality, domicile, residence or place of business of the user or of the data subjects concerned in the activity."[25] The US, or any country, could impose rules upon its nationals and corporations wherever they are handling information. If a corporation is doing business or has other contacts with a country, that country may attempt to impose regulations upon more than just local activity by the corporation.

3.9 ENFORCEMENT MACHINERY There are various mechanisms for the enforcement of data protection rules.

1. Private civil action.
2. Class actions.
3. Governmental civil action.
4. Criminal actions.
5. Administrative investigation and action. In the United States, the present political environment makes it unlikely that any new administrative or regulatory bodies or rules will be enacted. At the moment the argument that "regulation reduces production and increases inflation" has been widely accepted. However most other countries are creating new bureaucracies to attack the problem.

Penalties and remedies which may be applied include:

1. Damages -- direct, consequential, punitive, minimum, treble.
2. Attorney's fees
3. Jail or imprisonment
4. Elimination of the offending data.
5. Revocation of licenses to operate, either in whole or in part.
6. Revocation of professional certification for offending personnel.
7. Revocation of usage certification for software or hardware systems.
8. Fines
9. Injunctions (either requiring or prohibiting some action).
10. Contempt of court (civil or criminal).
11. Funding cut-off. For example, in the United States, the Federal medicaid program requires states to maintain certain records about individuals and restricts the disclosure of that information. If the state refuses to adhere to those rules or if they are violated, the Federal government

25. Sir Norman Lindop, chairman, Report of the Committee on Data Protection, October 1978, Cmnd. 7341. Section 18.46